

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(article 36 and regulation 70 of PCT)

Applicant or authorised representative file reference	FOR SUBSEQUENT ACTION		See international preliminary examination report transmission notification (form PCT/IPEA/416)
International application No. PCT/FR 03/01535	International filing date (day/month/year) 21.05.2003	Priority date (day/month/year)	05.06.2002
International patent classification (IPC) or both national classification and IPC H04L9/32			
Applicant FRANCE TELECOM et al.			

1.	This international preliminary examination report, drafted by the international preliminary examining authority, is forwarded to the applicant in accordance with article 36.		
2.	The REPORT comprises 5 pages, including this cover page.		
<input type="checkbox"/>	It is accompanied by APPENDICES, i.e. pages of the disclosure, claims or figures which have been amended and are used as a basis for this report or pages containing corrections made for the authority in charge of the international preliminary examination (see regulation 70.16 of instruction 607 of the administrative instructions of the PCT).		
	These appendices comprise _____ pages.		
3.	This report contains indications relating to the following points:		
I	<input checked="" type="checkbox"/>	Basis of report	
II	<input type="checkbox"/>	Priority	
III	<input type="checkbox"/>	No formulation of opinion with respect to novelty, inventive activity and possibility of industrial application	
IV	<input type="checkbox"/>	No invention unit	
V	<input checked="" type="checkbox"/>	Justified statement according to rule 66.2(a)(ii) with respect to novelty, inventive activity and possibility of industrial application; references and explanations to support this statement	
VI	<input type="checkbox"/>	Certain reference documents	
VII	<input type="checkbox"/>	Irregularities in international application	
VIII	<input type="checkbox"/>	Observations relating to international application	

International preliminary examination application submittal date 19.12.2003	Report completion date 10.11.2004
Name and postal address of international preliminary examining authority European patent office – PE 5619 Palentiaan 2 NL 2280 HV Rijswijk - Netherlands Tel. (+31) 70 340 – 2040 Tx: 31 651 epo nl Fax: (+31) 70 340 - 3016	Authorised official Holper, G Telephone No. +31 70 340-2304

I. Basis of report

1. Concerning **elements** of the international application (*replacement sheets that were submitted to the receiving office in response to an invitation made in accordance with article 14 are considered in this report as being "initially deposited" and are not attached to the report as an appendix since they do not contain any modifications*) (Regulations 70.16 and 70.17):

Disclosure, pages:

1-13 as initially deposited

Claims, No.:

1-14 as initially deposited

Drawings, sheets:

1/3-3/3 as initially deposited

2. Concerning the language, all elements mentioned above were available to the Authority or were submitted to the Authority in the language in which the International Application was deposited, unless mentioned otherwise under this point.

These elements were also available to the Authority or were submitted to the Authority in the following language: that is:

- the language of a translation submitted for the purposes of the international search (according to rule 23.1 (b)),
- the language in which the international application was published (according to regulation 48.3 (b)),
- the language of the translation submitted for the purposes of the international preliminary examination (according to regulation 55.2 or 55.3).

3. Concerning nucleotide or amino acid sequences divulged in the international application (if applicable), the international preliminary examination was carried out based on the listing of sequences:

- contained in the international application, in written form
- deposited with the international application, in a form that can be decrypted by computer,
- submitted to the Authority later, in written form,
- submitted to the Authority later, in a form that can be decrypted by computer,

- ☐ The declaration, according to which the listing of sequences in writing and supplied later does not go beyond the data divulged in the application as deposited, was provided,
- ☐ The declaration, according to which the information recorded in a form that can be decrypted by computer is identical to the listings of sequences in this document in writing, was provided,

4. The modifications cancelled:

- ☐ in the disclosure, pages:
- ☐ in the claims, numbers:
- ☐ in the figures, sheets:

5. ☒ This report was formulated making abstraction (of some) of the modifications, that were considered as going beyond the presentation of the invention as deposited, as mentioned below (regulation 70.2(c)):

(Any replacement sheet containing this type of modification must be indicated in point 1 and attached to this report).

6. Complementary observations if applicable:

V. Justified statement according to regulation 35(2) with respect to novelty, inventive activity and the possibility of industrial application; references and explanations to support this statement

- | | | | |
|---------------------------------------|------|--------|----------------|
| 1. Declaration | | | |
| Novelty | Yes: | Claims | 1-14 |
| | No: | Claims | |
| Inventive activity | Yes: | Claims | 3-7, 9 |
| | No: | Claims | 1, 2, 8, 10-14 |
| Possibility of industrial application | Yes: | Claims | 1-14 |
| | No: | Claims | |

2. References and explanations

See separate sheet

Concerning point V

Motivated declaration about the novelty, inventive activity and possibility of industrial application; quotations and explanations to support this declaration.

The following documents are referenced:

D1: US-B-6 215 872 B1 (VAN OORSCHOT PAUL C) April 10 2001 (2001-04-10)

D2: EP-A-0 856 821 (NIPPON TELEGRAPH & TELEPHONE) August 5 1998
(1998-08-05)

This application does not satisfy the conditions set down in article 33(1) in the PCT, since the subject of claims 1, 2, 8, 11-14 does not involve an inventive activity as defined in article 33(3) in the PCT.

Document D1 that is considered as being the state of the art closest to the subject of claim 1, describes a method for checking a digital signature involving a user comprising a data processing system (see col. 4, I.11-42; col. 5, I.2-5; col. 8, I.60 – col. 9, I.12; references between parentheses being applicable to this document), and the user receives requests to check digital signatures from the data processing system and processes these requests, a digital signature being generated using a private key known only to a signing entity and associated with a public key, comprising a storage step in a certificates table (trusted public key list 36) containing a digest form of at least one public key, and a digital signature checking phase comprising steps as follows: - receive the digital signature to be checked and a public key in a pair of keys including a private key that was used to generate the digital signature to be checked, - calculate a digest form of the received public key and search in the certificates table (36) for the calculated digest form of the public key, and – decrypt the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table.

Consequently, the only difference between the subject of claim 1 and this known process is that the method uses a microcircuit that can be connected to a data processing system and that the certificates table is stored in a memory in the microcircuit.

Therefore the problem that this invention as defined by claim 1 is intended to solve can be considered as being the practical embodiment of the known process. However, it is known that certificates and public keys can be stored in a memory of a smart card (see D2, fig. 4B, col. 5, I.57 – col. 6, I.29). Those skilled in the art would surely use such a card to perform the process according to D1 and would thus arrive at the subject of claim 1 without involving any inventive activity.

The same argument is applicable mutatis mutandis to the subject of the corresponding independent claims 13 and 14, which are therefore not inventive either.

The dependent claim 2 contains no additional characteristic that, in combination with claim 1, defines a subject that satisfies the requirements of article 33(3) PCT for the following reason:

the additional steps mentioned are equivalent to a conventional check of a received certificate; those skilled in the art would carry out this procedure before inserting a public key or its digest in order to guarantee authenticity of the received certificate

and would thus arrive at the subject of claim 2 without involving any inventive activity.

The dependent claims 8, 10, 11 and 12 do not contain any characteristic that, in combination with the characteristics of any of the claims to which they refer, defines a subject that satisfies the requirements of the PCT concerning the inventive activity, see documents D1 and D2 and the corresponding passages mentioned in the search report.

The combination of characteristics in claim 3 is not included in the state of the art and there is no obvious way of deriving it from the state of the art for the following reasons: no document in prior art divulges insertion of a pointer to the digest of the public key of the certification entity that issued a certificate, thus defining a certification tree stored in a memory of a microcircuit. Nor is the combination of the characteristics of claim 9 included in the state of the art, nor is it obviously derived from the state of the art.

Therefore, claims 3 and 9 satisfy the criteria of article 33(2) and (3) in the PCT.

Assuming that claims 4 – 6 are dependent on claim 3, they also satisfy the conditions required by the PCT as such concerning novelty and inventive activity.

Unlike the requirement of rule 5.1 a) ii) in the PCT, the description does not give the relevant state of prior art presented in documents D1 and D2 and does not mention these documents.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant:

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.